UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,499	02/28/2002	Zhichen Xu	100200290-1	7480

7590 11/17/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 11/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/084,499	XU ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) *31-41* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30 and 42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1 – 42 are pending.

Election/Restrictions

Claims 31 – 41 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected invention, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 9/6/2005.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 2, 8 – 13, 20 – 30, and 42 are rejected under 35 U.S.C. 102(b) as being anticipated by Goldschlag et al. (Goldschlag), "Hiding Routing Information".

Regarding claim 1, Goldschlag discloses:

forming a path from a provider to a requestor by selecting a plurality of peers in response to receiving a request for information (Goldschlag; page 2, par. 2 – page 3; page 4, par. 3)

updating a table on each peer of said plurality of peers with a respective path index entry for said information (Goldschlag, page 10, par. 4, lines 14-18);

transmitting a message to said requestor through said plurality of peers, said message comprising said information and a path index for said information from said provider; and determining a next peer according to said path for said information by searching said table of each peer of said plurality of peers with said path index as an index into said table (Goldschlag, page 11, par. 2).

Regarding claim 2, Goldschlag discloses:

retrieving an identity of said next peer according to said path for said information and a respective index peer of said next peer; encrypting said path index with a public key of said respective index peer of said next peer to form a next state of said path index; and transmitting a new message with said information and said next state of said path index as said path index to said next peer (Goldschlag, page 11; fig. 2; page 5, line 2).

Regarding claim 8, Goldschlag discloses:

forming a respective path message to each peer of said plurality of peers, said respective path message comprising said respective path index entry (Goldschlag, page 10, par. 4).

Regarding claim 9, Goldschlag discloses:

The method according to claim 8, wherein said respective path index entry comprises an identity of a next peer according to said path, a respective index peer for said next peer, and an index entry (Goldschlag, page 6, par. 1; page 10, par. 4).

Regarding claim 10, Goldschlag discloses:

wherein said identity of next peer according to said path and said respective index peer for said next peer are encrypted with a public key of a peer receiving said respective path message (Goldschlag, page 6, par. 1; page 10, par. 4).

Regarding claim 11, Goldschlag discloses:

wherein said index entry is formed according to [public.sub.b.sub..sub.j1(. . . public.sub.b.sub..sub.j1(public.sub.b.sub..sub.j0(n)) . . .)], where b.sub.j represents said respective index peer (Goldschlag, fig. 2; page 5, line 2; fig. 4).

Regarding claim 12, Goldschlag discloses:

updating a respective table of each peer of a plurality of peers with a respective path index entry in response to receiving a path formation message containing said

respective path index entry (Goldschlag; page 2, par. 2 – page 3; page 4, par. 3; page 10, par. 4, lines 14-18);

receiving a message comprising said information and a path index; and forwarding said information to a next peer in response to a determination of said next peer from said table with said path index as a search index into said table (Goldschlag, page 11, par. 2).

Regarding claim 13, it is rejected, at least, for the same reasons as claim 2.

Regarding claim 20, Goldschlag discloses:

receiving said message at said requestor; applying a complementary key to said public key of said requestor to said encryption key encrypted with said public key of said requestor to obtain said encryption key; applying said encryption key to said encrypted reference to retrieve said information (Goldschlag, page 6, par. 2; page 11, par. 2).

Regarding claim 21, Goldschlag discloses:

selecting a path for information from a provider to a requestor through a plurality of peers in response to a received request for said information; and receiving a respective set-up message at each peer of said plurality of peers, wherein said respective set-up message comprises a predetermined label and an identity of a next peer for said information according to said path (Goldschlag, page 6, par. 1).

Regarding claim 22, it is rejected, at least, for the same reasons as claim 1.

Regarding claim 23, Goldschlag discloses:

receiving a message, wherein said message comprises: an encryption key encrypted with a public key of said requestor; said information encrypted with said encryption key; and a message label; and retrieving said identity of next peer from said table in response to said message label matching said predetermined label in said table (Goldschlag, page 8, par. 1; page 11, par. 2).

Regarding claim 24, it is rejected, at least, for the same reasons as claim 2.

Regarding claim 25, Goldschlag discloses:

comparing said identity of said next peer with a current peer; decrypting said encryption key encrypted with a public key of said requestor in response to said identity of said next peer being said current peer; and decrypting said information encrypted with said encryption key (Goldschlag, page 11, pars. 1,2).

Regarding claim 26, Goldschlag discloses:

generating an encryption key; encrypting said encryption key with a public key of said requestor; encrypting said encryption key with a public key of said provider; and encrypting a transaction identifier, a reference for said information, and a first next peer according to said path with said encryption key (Goldschlag, page 8, par. 1; page 11, pars. 1, 2).

Regarding claim 27, Goldschlag discloses:

forming a retrieval message comprising: said encryption key encrypted with said public key of said requestor; said encryption key encrypted with said public key of said provider; said transaction identifier, said reference for said information, and said first next peer according to said path encrypted with said encryption key; and transmitting said retrieval message to said provider (Goldschlag, pages 4, 5; page 6, pars. 1,2; page 8, par. 1; page 11, pars. 1, 2).

Regarding claim 28, Goldschlag discloses:

applying a complementary key of said provider to said encryption key encrypted with said public key of said provider; and decrypting said reference for said information, said transaction identifier, and said first next peer (Goldschlag, page 6, pars. 1, 2).

Regarding claim 29, Goldschlag discloses:

retrieving said information based on said reference for said information; encrypting said information with said encryption key; and forming a message label based on said transaction identifier (Goldschlag; page 2, par. 2 – page 3; page 4, par. 3; page 8, par. 1; page 10, par. 4; page 11, pars. 1,2).

Regarding claim 30, Goldschlag discloses:

forming a message including said encrypted information and said message label; and transmitting said message to said first next peer (Goldschlag, page 11, pars. 1,2).

Regarding claim 42, it is rejected, at least, for the same reasons as claims 2, 13, and 22.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3 – 7 and 14 – 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goldschlag in view of Clarke et al. (Clarke), "Freenet: A Distributed Anonymous Information Storage and Retrieval System".

Regarding claim 3, Goldschlag discloses a system for requesting and retrieving information on a network. The system employs a method for hiding the path (creating an anonymous connection) for such requests and replies (Goldschlag, pages 1-3). Goldschlag discloses the receiving of a request for information, and the formation of a path to said requested information (see rejection of claim 1). Goldschlag, however,

does not disclose that the reception for a request for information was at a directory, a determination of availability, or a notification of non-availability.

Clarke similarly discloses a system for requesting and retrieving information, anonymously, on a network. More specifically, Clarke discloses methods for requesting and receiving information, where the information consists of file transactions (Clarke, page 2, par. 1). Because onion routing systems, such as disclosed by Goldschlag, do not focus on the publication, access, and storage of files, Clarke discloses that this system is "best viewed as a complement" to such a onion routing system. Clarke discloses that an additional advantage of such a combination is increased security (Clarke, page 17, table 1, pars. 1-4).

It would have been obvious to one of ordinary skill in the art to employ the methods of Clarke within the system of Goldschlag. This would have been obvious because one of ordinary skill in the art would have known the explicit teachings for the combination of these systems, as well as recognized the benefits of additional security.

Thus, the combination of Goldschlag and Clarke disclose:

receiving said request for information at a directory (Clarke, page 3, par. 3, lines 1-6; page 18, lines 2-6; page 18, par. 2; page 4, pars. 1, 2). Clark discloses that each node acts as a directory containing the locations to requested files.

determining an availability of said information (Clarke, page 6, par. 4);

and notifying said requestor of a determination of non-availability (Clarke, page 6, par. 4). The combination of Goldschlag and Clarke discloses that the method includes notifying the requestor of a decision ("determination") of the quality or state of being

non-available ("non-availability") of the requested file. In this case, if the file is available, the method notifies the requester that the file is available - a decision of non-affirmation regarding the quality of the file being non-available. Furthermore, the combination of Goldschlag and Clarke discloses that the method includes notifying a requester that it has been determined that a file is not available on a particular node (Clarke, page 6, par. 5, lines 3,4).

Regarding claim 4, the combination of Goldschlag and Clarke disclose:

receiving said request for information at a directory (Clarke, page 3, par. 3, lines 1-6; page 18, lines 2-6; page 18, par. 2; page 4, pars. 1, 2). The combination of Goldschlag and Clarke discloses that each node acts as a directory containing the locations to requested files.

determining an availability of said information (Clarke, page 6, par. 4);

and generating an encryption key in response to a determination of said availability (Clarke, page 3, par. 3, lines 1-6; page 18, lines 2-6; page 18, par. 2; page 4, pars. 1, 2). The combination of Goldschlag and Clarke discloses that when a file is found to be available on a remote node, the request for the file if forwarded to the remote node. When such requests are forwarded, the combination of Goldschlag and Clarke discloses that these requests are link encrypted with an encryption key. The process of encrypting a request with an encryption key clearly results in the process of coming into being (the "generation") of an encryption key, whether the key is produced

from storage, received over a network, or the resultant of a key-derivation algorithm (Goldschlag, fig. 1; page 10, par. 3).

Regarding claim 5, the combination of Goldschlag and Clarke disclose: *determining a first next peer from said provider and a respective index peer for said first next peer according to said path; and encrypting a reference to said information, said first next peer, and said respective index peer of said first next peer with said encryption key* (Goldschlag, page 6, par. 1).

Regarding claim 6, the combination of Goldschlag and Clarke disclose: *wherein said encryption key is generated according to a DES encryption algorithm.* Goldschlag discloses using a efficient symmetric algorithm for the encryption key, however, Goldschlag does not specify DES encryption. It would have been obvious to use DES encryption as this is an efficient algorithm used in the onion routing system as evidenced by Goldschlag, "Anonymous Connections and Onion Routing", page 6, section E – Onions).

Regarding claim 7, the combination of Goldschlag and Clarke disclose: *encrypting said encryption key with a public key of said requestor; encrypting said encryption key with a public key of said provider; forming a provider message, wherein said provider message comprises: said encryption key encrypted with said public key of said requestor; said encryption key encrypted with said public key of said*

provider; said encrypted reference; and said encrypted first next peer and said respective first index peer; and transmitting said message to said provider (Goldschlag, page 6, section 3.1).

Regarding claim 14, it is rejected, at least, for the same reasons as claim 3.

Regarding claim 15, it is rejected, at least, for the same reasons as claims 4 and 5.

Regarding claim 16, it is rejected, at least, for the same reasons as claims 4 – 7.

Regarding claim 17, it is rejected, at least, for the same reasons as claim 6.

Regarding claim 18, the combination of Goldschlag and Clarke disclose:

receiving said second message at said provider; applying a complementary key to said public key of said provider to said obtain said encryption key; and applying said encryption key to said encrypted reference to retrieve said reference (Goldschlag, page 6, section 3.1).

Regarding claim 19, it is rejected, at least, for the same reasons as claim 7, and furthermore because the combination of Goldschlag and Clarke disclose the retrieving

of information based upon a reference (a request for said information) (Clarke, section 3.2).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Goldschlag et al., "Anonymous Connections and Onion Routing", May 1998, IEEE Journal on Selected Areas in Communication, Vol. 16, No. 4.

Claessens et al., "Solutions for Anonymous Communication on the Internet", 1999, IEEE ICCST.

Goldschlag et al., "Onion Routing for Anonymous and Private Internet Connections", Feb. 1999, Communications of the ACM, Vol. 42, No. 2.

Goldschlag et al., "Onion Routing Access Configurations", Jan. 2000, DARPA Information Survivability Conference and Exposition, DISCEX '00. Proceedings, Volume 1, Page(s):34 - 40.

A shortened statutory period for reply is set to expire **3** months (not less than 90 days) from the mailing date of this communication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
Assistant Examiner
Art Unit 2137

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137